



CHAPTER 2

Cisco TrustSec ソリューションの設定

この章では、次の事項について説明します。

- 「設定の概要」(P.2-1)
- 「デフォルト設定」(P.2-3)
- 「その他のマニュアル」(P.2-3)

設定の概要

このマニュアルは、Cisco Catalyst スイッチの基本的な Cisco TrustSec 設定手順を説明し、TrustSec コマンドリファレンスが含まれます。

ネットワーク全体の導入設定については、[Cisco TrustSec 設定のハウツー マニュアル](#)のセクションを参照してください。

ネットワーク全体の導入には、Cisco Identity Services Engine (Cisco ISE)、Cisco Secure Access Control System (Cisco ACS)、Cisco IP Phone、シスコのルータ、シスコのネットワーク機器などの、複数のデバイスの設定、相互運用性と管理が含まれています。

Cisco TrustSec Solution を説明するホワイトペーパーとプレゼンテーションは次の URL にあります。
<http://www.cisco.com/en/US/netsol/ns1051/index.html>

Cisco TrustSec 設定のハウツー マニュアル

一連の「ハウツー」コンフィギュレーション マニュアルは、複雑なシナリオで実績のあるネットワーク アーキテクチャを実現するための導入ガイドラインとベストプラクティスについて説明します。Cisco TrustSec の「ハウツー」マニュアルは、すべて次の URL にあります。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

『TrustSec 2.1 Configuration How-to Guide』には次のトピックが含まれます。

- 概要
- 計画と導入前チェック リスト
- ISE の基本設定 : ISE のブートストラップ
- ID ストアの追加と認証の作成
- グローバル スイッチの設定
- Wireless LAN Controller の基本設定
- 段階的な導入の概要

- モニタ モード
- モニタ モードからの移行
- ロー インパクト モード
- クローズド モード
- ISE プロファイリング サービス
- ISE の基本設定: 無差別 VMware
- 中央 Web 認証
- 複数の Active Directory ドメインに対するユーザ認証および認可
- ISE の導入タイプおよびガイドライン
- アクセスを区別する証明書の使用
- オンボーディングおよびプロビジョニング
- セキュリティ グループ アクセスを使用したサーバ間セグメンテーション
- AnyConnect NAM と Cisco ISE を使用した EAP の連結の導入
- 失敗した認証および認可

サポート対象ハードウェアおよびソフトウェア

TrustSec リリースごとの TrustSec のサポート対象ハードウェアとソフトウェアの一覧については、次を参照してください。

次の URL の『*Release Notes for Cisco TrustSec General Availability Releases*』

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

ご使用のデバイスのリリース ノート、コンフィギュレーション ガイド、コマンドリファレンスも参照してください。

Cisco TrustSec の前提条件

次に、Catalyst スイッチで TrustSec ネットワークを構築するための前提条件を示します。

- すべてのネットワーク デバイスの TrustSec ソフトウェア
- すべてのネットワーク デバイス間の接続
- TrustSec ライセンスで動作する Cisco Secure ACS 5.1 または Cisco ISE のネットワークの可用性
- ネットワーク上で機能するディレクトリ、DHCP、DNS、認証局および NTP サーバ

Cisco TrustSec の注意事項および制限事項

Catalyst スイッチの Cisco TrustSec に関する次のガイドラインおよび制限があります。

- Cisco TrustSec の AAA は RADIUS を使用し、Cisco Secure Access Control System (ACS) バージョン 5.1 以降のみでサポートされています。
- NDAC 認証を実行するには Cisco TrustSec で 802.1X 機能をグローバルにイネーブルにする必要があります。802.1X をグローバルにディセーブルにすると、NDAC はディセーブルにあります。
- Cisco TrustSec は物理インターフェイスだけでサポートされ、論理インターフェイスでサポートされません。
- Cisco TrustSec はこのガイドで参照されているリリースでは IPv6 をサポートしていません。
- スイッチにデフォルトのパスワードが実装されている場合、そのスイッチでの接続は、デフォルトパスワードを使用するようにパスワードを設定する必要があります。デフォルトのパスワードが設定されていない場合、そのスイッチでの接続はパスワード設定を使用しないように設定してください。パスワードオプションの設定は導入ネットワーク全体で一貫している必要があります。
- 異なるスイッチ上の異なる値には **retry open timer** コマンドを設定します。

デフォルト設定

表 2-1 に Cisco TrustSec パラメータのデフォルトの設定値を示します。

表 2-1 Cisco TrustSec パラメータのデフォルト値

パラメータ	デフォルト
Cisco TrustSec	ディセーブル。
SXP	ディセーブル。
SXP デフォルト パスワード	なし。
SXP の復帰期間	120 秒 (2 分)
SXP リトライ期間	60 秒 (1 分)
Cisco TrustSec のキャッシング	ディセーブル。

その他のマニュアル

リリース固有のドキュメント

リリース固有のドキュメントのタイトル	TrustSec トピック
『Release Notes for Cisco TrustSec General Availability Releases』	<ul style="list-style-type: none"> • オープンおよび解決済みの注意事項 • 現在のハードウェアおよびソフトウェアのサポート

プラットフォーム固有のマニュアル

プラットフォーム固有のマニュアルのタイトル	TrustSec トピック
Catalyst 3000 シリーズ スイッチ	
『Release Notes for Catalyst 3560 and 3750 Switches』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 3560 Software Configuration Guides』	802.1x 設定手順
『Catalyst 3750-E and 3560-E Switch Software Configuration Guide』	
『Cisco Catalyst 3560-X Series Switches Software Configuration Guides』	
『Catalyst 3750 Metro Series Switches Software Configuration Guides』	
『Cisco Catalyst 3750-X Series Switches Software Configuration Guides』	
Catalyst 4500 シリーズ スイッチ	
『Cisco Catalyst 4500 Series Switches Release Notes』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 4500 Series Switches Software Configuration Guides』	802.1x 設定手順
Catalyst 6500 シリーズ スイッチ	
『Cisco Catalyst 6500 Series Switches Release Notes』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide』	802.1x 設定手順
『Catalyst 6500 Release 12.2SY Software Configuration Guide』	
『Catalyst 6500 Release 15.0SY Software Configuration Guide』	
Nexus 7000 シリーズ スイッチ	
『Cisco Nexus 7000 Series Switches Release Notes』	オープンおよび解決済みの注意事項
『Cisco Nexus 7000 Series Switches Configuration Guides』	<ul style="list-style-type: none"> • Cisco Nexus 7000 シリーズ スイッチ、リリース 4.1 以降の TrustSec 機能の設定 • 802.1X 設定手順
Cisco Secure Access Control System および Cisco Identity Services Engine	
『Cisco Secure Access Control System Release Notes』	オープンおよび解決済みの注意事項
『Cisco Secure Access Control System End-User Guides』	Cisco ACS 5.1 以降の TrustSec の設定
Cisco Identity Services Engine	TrustSec の設定。ISE のマニュアルでは、TrustSec は SGA、またはセキュリティ グループ アクセスと呼ばれます。

Cisco IOS ソフトウェア マニュアル セット

Cisco IOS マニュアルのタイトル	TrustSec トピック
『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.2SX』	802.1x、SXP、L2 SGT インポジションの設定手順
『Securing User Services Configuration Guide Library, Cisco IOS Release 15.2S』	

